

SEALED

United States District Court

FILED**MAY 18 2015**

CLERK, U.S. DISTRICT COURT

By

DISTRICT OF

Deputy

NORTHERN

TEXAS

In the Matter of the Search of

(Name, address or Brief description of person, property or premises to be searched)

AER51054@gmail.com

APPLICATION AND AFFIDAVIT

FOR SEARCH WARRANT

CASE NUMBER: *B:15m; 334-BN*

I, Carlos Hernandez, being duly sworn depose and say:

I am a(n) Special Agent with the Drug Enforcement Agency and have reason to believe that on the property known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of
TEXAS

there is now concealed a certain person or property, namely (describe the person or property to be seized)

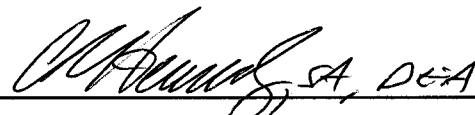
(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, concerning a violation of Title 21 United States code, Section(s) 841 and 846. The facts to support a finding of Probable Cause are as follows:

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT Carlos Hernandez)

Continued on the attached sheet and made a part hereof.

☒ Yes ☐ No

Signature of Affiant

Carlos Hernandez

Special Agent, DEA

Sworn to before me, and subscribed in my presence

5/18/2015

Date

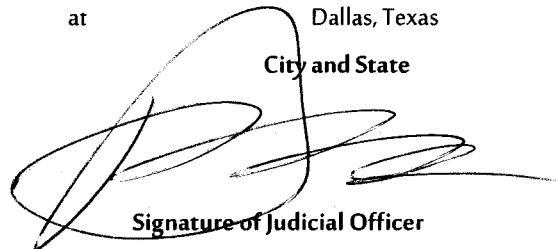
DAVID L. HORAN

United States Magistrate Judge

Name and Title of Judicial Officer

at Dallas, Texas

City and State



Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH:)
{AER51054@gmail.com} THAT IS)
STORED AT PREMISES CONTROLLED)
BY GOOGLE, INCORPORATED)

FILED UNDER SEAL

AFFIDAVIT

I, Carlos R. Hernandez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Google Incorporated (hereinafter referred to as Google), an electronic mail (email) provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A, which is incorporated by reference. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2320(a) to require Google Incorporated to disclose to the government, records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7); that is, I am an officer of the United States who is authorized by law to conduct investigations and make arrests for offenses

enumerated in 18 U.S.C. § 2516. I have been employed as a Special Agent with the United States Department of Justice, Drug Enforcement Administration (DEA), Dallas Field Division, since August 1997. Prior to working for the DEA, I was employed as a Special Agent with the United States Air Force Office of Special Investigations for over seven years. I am currently assigned to the North Texas High Intensity Drug Trafficking Area. I have received extensive training on how to conduct narcotics investigations and have participated in these types of investigations for the past seventeen years. I have used a variety of methods to investigate narcotic organizations including, but not limited to, electronic surveillance, visual surveillance, general questioning of witnesses, the use of search warrants, the use of confidential informants, the use of pen registers, and the use of undercover agents. I have also received specialized training in Title-III interceptions from the DEA.

3. I am familiar with the facts and circumstances of the investigation set forth below through my personal participation; from discussions with other federal agents and local law enforcement officers; and from my review of records and reports relating to the investigation.

4. I am currently conducting an investigation involving the online activities of e-mail address AER51054@gmail.com ("**Target Account**"). There is probable cause to believe that Manuel Montero-Orozco used the **Target Account** in furtherance of violations of federal law, including 21 U.S.C. §§ 841(a)(a), 21 USC 843, and 21 USC

846, and that evidence, fruits, and instrumentalities of those violations (as described in Attachment B) will be found therein.

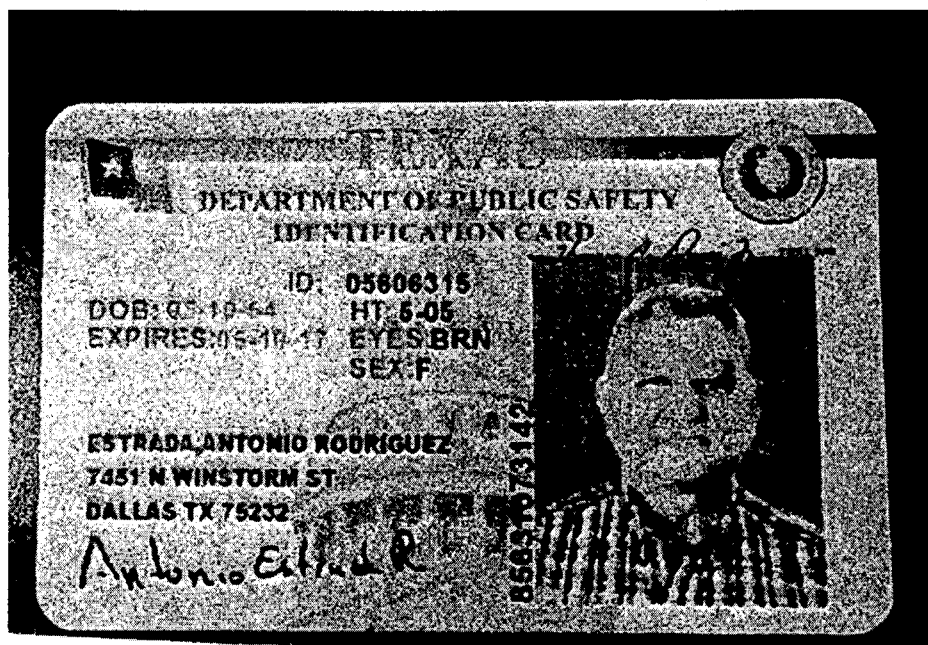
PROBABLE CAUSE

5. Affiant has been investigating the drug-trafficking activities of Ignacio Andrade-Lopez and his drug-trafficking organization suspected to be distributing multi-pound quantities of methamphetamine in the Dallas, Texas area. On April 6, 2015, Manuel Montero-Orozco was arrested based on federal complaint #3:15MJ215-BN, in the Northern District of Texas, Dallas, Texas following the execution of a search warrant at 646 Meadowglen Drive, Duncanville, Dallas County, Texas.

6. On January 21, 2015, Ignacio Andrade-Lopez sold approximately one pound of methamphetamine to an undercover officer in Grand Prairie, Dallas County, Texas. In the weeks following this event, Andrade-Lopez was followed to numerous locations suspected of being drug stash locations and drug processing labs. Two of the locations were 646 Meadowglen Drive, Duncanville, Texas and 717 NW 14th Street, Grand Prairie, Texas. Following the development of additional evidence, on April 2, 2015, federal search warrant #3:15MJ210-BN, was signed and authorized by United States Magistrate Judge David L. Horan, U.S. District Court, Northern District of Texas for the residence at 646 Meadowglen Drive, Duncanville, Texas. Approximately six kilograms of methamphetamine, a stolen handgun, and numerous documents among other things were seized from the house. Wilber Farias-Lopez and Manuel Montero-Orozco were arrested

at that time and later charged by complaint with drug offenses in the Northern District of Texas

7. Among the documents seized from the residence at 646 Meadowglen Drive were printed emails between Tomas Rodriguez, a realtor, and Nancy Boliver, a representative of Leap Property Management, regarding a pending rental agreement between Anthony Rodriguez and Leap Property Management. Also seized from the residence were the rental agreements for 646 Meadowglen Drive and 717 NW 14th Street, Grand Prairie, Texas, and a Texas state identification card in the name of Antonio



Estrada-Rodriguez.

8. This card has a picture of Manuel Montero-Orozco. A check of Texas Department of Public Safety databases revealed the card uses a number assigned to a different person, and lacks information and markings which should appear on proper ID cards. Further, the subject's sex is indicated to be female. A note attached to one of the emails has the **Target Account** and password handwritten on it as well as a telephone

number, 214-931-0491 described on the note as, "phone # associated with Acct."

1/31/2015

Gmail - Your Application Fee Receipt



Antonio Rodriguez <aer51054@gmail.com>

Your Application Fee Receipt

LEAP Property Management <nboliver@leapdfw.com>

Sat, Jan 31, 2015 at 12:34 AM

Reply-To: nboliver@leapdfw.com

To: AER51054@gmail.com

Dear ANTONIO E. Rodriguez,

Your rental application fee payment has been processed. You will see a charge from "AF*LEAP Property Mana." on your credit or debit card statement.

The details of your payment are as follows:

Card Number:9038

Card Type: Visa

Amount: \$45.00

Paid On: 01/31/2015 12:34 AM (CST)

Confirmation Number: AYF0-YHBI

[Click here to view the listing.](#)

Thank you,
LEAP Property Management
(940) 566-6413

firstunitedbank.com	
GMAIL	
Account	
AER 51054	USER NAME
1234@5678@PW	PassWord
214-931-0491 phone # associated with Acct	

9. On September 2, 2015, Yesenia Robles, the wife of Ignacio Andrade-Lopez, was interviewed by agents. She identified telephone number 214-931-0491 as a telephone number belonging to her husband (Ignacio Andrade-Lopez). Another document found with the rental agreements was a printed copy of an email from nboliver@leapdfw.com to the **Target Account**. The email is a receipt for a rental application fee of \$45.00.

10. Affiant knows from his experience and training that individuals engaged in drug trafficking activities such as Andrade-Lopez and Montero-Orozco are in constant need of locations for storing and processing of drugs and weapons, and therefore rent properties under assumed names to avoid detection by law enforcement. In this instance, there is reason to believe this drug trafficking organization used and possibly continues to use the **Target Account** to facilitate the acquisition of these properties.

11. On about April 15, 2015 a preservation letter was served on Google Incorporated for the **Target Account**.

GOOGLE APPLICATIONS OVERVIEW

12. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel with whom I have spoken, I know that:

13. Datacenters are facilities used to host computer systems and telecommunications along with internet servers. Google's datacenters are located around the world in places such as Berkeley County, South Carolina; Council Bluffs, Iowa; Hamina, Finland; and St. Ghislian, Belgium.

14. Google provides email services, known as Gmail, which are available free of charge to Internet users. Subscribers obtain an account by registering on the Internet with Google. Google requests subscribers to provide basic information such as name, gender, zip code, and other personal/biographical information. However, Google does not verify the information provided.

15. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information.

16. Subscribers to Gmail may access their accounts on servers maintained and/or owned by Google from any computer connected to the Internet located anywhere in the world.

17. Any email that is sent to a Google subscriber is stored in the subscriber's "mailbox" on the provider's servers until the subscriber deletes the email or the subscriber's mailbox exceeds storage limits preset by Google. If the message is not deleted by the subscribers, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the providers' servers indefinitely.

18. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers and then transmitted to its end destination. Users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely. The sender can delete the stored email message thereby eliminating it from the email box maintained at the provider, but that message will remain in the recipient's email box unless the recipient deletes it as well or unless the recipient's account is subject to the account's limitations.

19. A Gmail subscriber can store files, including emails and image files, on servers maintained and/or owned by the provider, so emails and image files stored by a

Gmail subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store emails and/or other files on the provider's server when there is insufficient storage space in the subscriber's computer and/or when he/she does not wish to maintain them in the computer in his/her residence. A search of the files in the computer in the subscriber's residence, or in a portable computer, will not necessarily uncover the files that the subscriber has stored on the Gmail server.

20. In my training and experience, I have learned that Google provides a variety of other on-line services, including {fill in details of Google service to search, such as Google +, Hangouts, Drive, Maps, etc.}.

21. In general, email providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

22. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses

associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

23. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

GOOGLE SEARCH PROCEDURES

25. In order to ensure that agents search only those computer accounts and/or files described herein and in Attachment A, this affidavit and application for search warrant seeks authorization to permit employees of Google to assist agents executing this warrant to search only those computer accounts and/or files described in Attachment A.

The following procedures will be implemented:

- a. The search warrant will be presented to Google personnel who will be directed to isolate these accounts and files described in Attachment A.

- b. In order to minimize any disruption of computer service to innocent third parties, Google employees trained in the operation of computers will create an exact duplicate of the computer accounts and files described below, including an exact duplicate of all information stored in the computer accounts or files described below.
- c. Google personnel will provide the exact duplicate of the accounts and files described below, and all information stored in those accounts and/or files to the Special Agent who serves this search warrant.
- d. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Google for evidentiary purposes.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

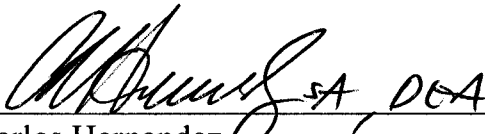
CONCLUSION

27. Based on the forgoing, I request this Court issue this search warrant for information associated with **AER51054@gmail.com** as there is probable cause to believe

that the user of the account has used it to commit violations of 21 U.S.C. §§ 841(a)(a), 21 USC 843, and 21 USC 846. There is also probable cause to believe evidence, instrumentalities and contraband will be located in information association with **AER51054@gmail.com**.

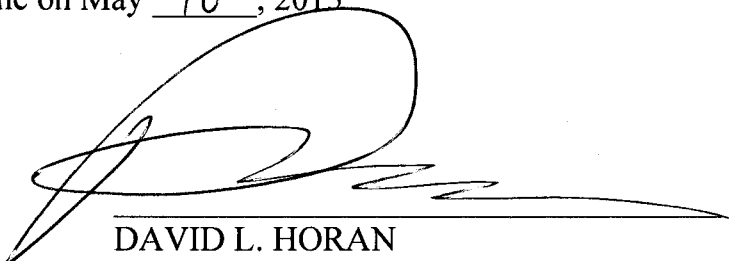
28. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court (including a magistrate judge of such a court) of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



Carlos Hernandez
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me on May 18, 2015



DAVID L. HORAN
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF TEXAS

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **AER51054@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google Incorporated, a company headquartered at 1600 Amphitheater Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, instant messaging, chats, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, to include email content stored in domain-based email accounts hosted on Google within the last ninety days;

b. Any deleted emails, including any information described in subparagraph “a.” above.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of

service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- d. The types of service utilized;
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy (friends) lists to include Google IDs, calendar data, pictures, and files;
- f. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.
- g. Any and all contents of electronic files that the subscriber has stored in the subscriber's Briefcase and/or Flickr account.

II. Information to be seized by the government

- a. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, Google conversations, and electronic messages that constitute evidence, contraband, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(a), 21 USC 843, and 21 USC 846

including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

b. Electronic communications involving the trafficking in illegal drugs or soliciting or producing pornographic images of minors or arranging meetings with minors.

c. Electronic communications involving laundering the proceeds of trafficking in illegal drugs.

d. Records relating to who created, used, or communicated with the TARGET ACCOUNT including identifying records disclosing the user's identity, and whereabouts (including, specifically, logs of IP addresses associated with each stored electronic communication).

e. Credit card and other financial information including but not limited to bills and payment records;

f. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A;

g. Evidence of the times the account or identifier listed on Attachment A was used;

h. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts